

A positive solution to Hilbert's 10th problem

Michael Pfender*

April 2014
last revised July 18, 2014

Abstract

Polynome codes and code evaluation; arithmetical theory frames; μ -recursive race for decision; decision correctness; decision termination in Zermelo-Fraenkel set theory ZFC+ with axiom of choice and consistency provability; decision correctness in theory $\mathbf{T} = \mathbf{PR}$ of Primitive Recursion; comparison with the negative result of Matiyasevich; positive solution for each single diophantine polynomial in *p. r. non-infinite-descent theory* $\pi\mathbf{R} = \mathbf{PR} + (\pi)$.

Contents

1 Hilbert's 10th Problem	3
2 Polynome coding and code evaluation	4
3 Arithmetical frame theories	5

*michael.pfender@alumni.tu-berlin.de

4	A μ -recursive race for decision	6
5	Decision Correctness	9
6	Termination	10
7	Correct termination of decision ∇	12
8	Comparison with Matiyasevich's negative result	13
9	Hilbert 10 constructively	14
9.1	Decision Correctness	16
9.2	Decision Termination	18

Introduction

Within theory $\mathbf{ZFC}^+ = \mathbf{ZFC} + \text{Con}_{\mathbf{ZFC}}$ of Zermelo-Fraenkel **set** theory with axiom of choice **AC**, strengthened by formula $\text{Con}_{\mathbf{ZFC}}$ which is to express \mathbf{ZFC} 's *internal, gödelised* consistency, we solve Hilbert's 10th problem positively: we organise decision of diophantine polynome codes—decision on overall *non-nullity*—as an enumerative μ -recursive race for a (first) zero (*counterexample*), against race for a first internal \mathbf{ZFC} -non-nullity *proof* for a given such polynomial code, given as the (nested) list of coefficients. Comparison with Matiyasevich's negative solution of Hilbert's 10th problem gives inconsistency of theory $\mathbf{ZFC} + \text{Con}_{\mathbf{ZFC}}$ whence self-inconsistency $\mathbf{ZFC} \vdash \neg \text{Con}_{\mathbf{ZFC}}$.

In a final section we plug our positive solution of the problem into the constructive framework of *p. r. non-infinite descent theory* $\pi\mathbf{R} = \mathbf{PR} + (\pi)$ out of *Arithmetical Foundations* in the References.

This is to give a decision algorithm for each single diophantine equation (in a uniform way), as asked in the original Hilbert’s 10th problem.

1 Hilbert’s 10th Problem

We attempt a positive solution to Hilbert’s 10th problem. In its original form it reads:

10. DETERMINATION OF THE SOLVABILITY OF A DIOPHANTINE EQUATION Given a diophantine equation with any number of unknown quantities and with rational integer numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

[translation quoted from MATIYASEVICH 1993.]

Formally, this text allows for a separate decision algorithm (“process”) for each diophantine polynomial. But it is clear that a decision-*family* must be *uniform* in a suitable sense.

Correctness of our alleged μ -recursive decision algorithm $\nabla_{\mathbf{ZFC}} : \text{DIO} \rightarrow 2 = \{0, 1\}$ builds, within \mathbf{ZFC}^+ , on diophantine soundness inferred by $\text{Con}_{\mathbf{ZFC}}$ over \mathbf{ZFC} . Termination follows from (countable) Choice. This already within \mathbf{ZFC} . Together this gives the wanted decision $\nabla = \nabla_{\mathbf{ZFC}}$ within \mathbf{ZFC}^+ , of all polynome codes in $\text{DIO} \subset \mathbb{N}$.

Comparison with Matiyasevich’s negative Theorem, *unsolving* Hilbert’s 10th Problem, theorem in particular of (classically quantified Arithmetical Theory) \mathbf{ZFC}^+ , gives a contradiction within \mathbf{ZFC}^+ , hence self-inconsistency of \mathbf{ZFC} , and from that in particular ω -inconsistency.

In a final section we show correctness and irrefutable termination of *localised* decision $\nabla[D]$ —for each single diophantine

polynomial $D = D(\vec{x})$ —within the constructive framework of p. r. *finite-descent-theory* $\pi\mathbf{R} = \pi\mathbf{R} + \text{Con}_{\pi\mathbf{R}}$ out of op. cit.

2 Polynome coding and code evaluation

Diophantine polynomials $D = D(\vec{\xi}) : \mathbb{Z}^* \rightarrow \mathbb{Z}$ (“in **DIO**”) are $\text{\LaTeX}/\text{\texttt{ASCII}}$ coded into

$$\text{DIO} =_{\text{def}} \mathbb{Z}^{(*)} \cong \bigcup_{m \geq 1} \mathbb{Z}[\xi_1, \dots, \xi_m] = \bigcup_{m \geq 1} \mathbb{Z}[\xi_1][\xi_2] \dots [\xi_m]$$

as nested coefficient *lists* $\mathbb{Z}^{(*)} \subset \mathbb{N}$.

[The symbols ξ_i are the *indeterminates*.]

Example:

$$\begin{aligned} D = D(\xi_1, \xi_2) = & (2 \cdot \xi_1^0 + 3 \cdot \xi_1^1 - 4 \cdot \xi_1^3) \cdot \xi_2^0 \\ & + (0 \cdot \xi_1^0 + 3 \cdot \xi_1^1 - 7 \cdot \xi_1^2) \cdot \xi_2^1 + (1 - 4 \cdot \xi_1) \cdot \xi_2^2 \end{aligned}$$

is coded 1-1 as (nested) coefficient list

$$\begin{aligned} \lrcorner D \lrcorner &= \langle \langle 2; 3; 0; 4 \rangle; \langle 0; 3; -7 \rangle; \langle 0 \rangle; \langle 1; -4 \rangle \rangle : \\ \mathbb{1} \rightarrow \text{DIO} &=_{\text{by def}} \mathbb{Z}^{(*)} \subset \mathbb{N} : \\ &\text{defined element, point of DIO} \end{aligned}$$

PR evaluation of DIO codes:

Evaluation $\text{ev} = \text{ev}(d, \vec{x}) : \text{DIO} \times \mathbb{Z}^*$ is PR defined

$$\begin{aligned} \text{ev}(d, \langle \vec{x}; x_{m+1} \rangle) &= \text{ev}(d, \langle x_1; \dots; x_m; x_{m+1} \rangle) \\ &=_{\text{def}} \text{ev}(\text{horner}(d, x_{m+1}), \langle \vec{x} \rangle) : \\ \text{DIO} \times \mathbb{Z}^* \supset \mathbb{Z}[\vec{\xi}, \xi_{m+1}] \times \mathbb{Z}^{m+1} &\xrightarrow{\cong} (\mathbb{Z}[\vec{\xi}][\xi_{m+1}] \times (\mathbb{Z}^m \times \mathbb{Z})) \\ &\xrightarrow{\cong} (\mathbb{Z}[\vec{\xi}][\xi_{m+1}] \times \mathbb{Z}) \times \mathbb{Z}^m \xrightarrow{\text{horner} \times \text{id}} \mathbb{Z}[\vec{\xi}] \times \mathbb{Z}^m \xrightarrow{\text{ev}} \mathbb{Z}, \end{aligned}$$

recursively by iterative application of Horner's schema to the hitherto trailing argument, until all of the arguments (constants or variables) are substituted into their corresponding indeterminates ξ_j .

Result then is the integer $\text{ev}(d, \vec{x})$, constant or integer variable.

For the **example** above, $D = D(\xi_1, \xi_2)$, with argument string $\langle x_1; x_2 \rangle := \langle 23; 64 \rangle \in \mathbb{Z}^*$, we get

$$\begin{aligned} \text{ev}(d, \langle x_1; x_2 \rangle) &= \text{ev}(\langle \langle 2; 3; 0; 4 \rangle; \langle 0; 3; -7 \rangle; \langle 0 \rangle; \langle 1; -4 \rangle \rangle, \langle 23; 64 \rangle) \\ &= \text{horner}(\(((((-4 \cdot 64 + 1) \cdot \xi_1 + 0)) \cdot \xi_1 + (-7 \cdot 64 + 3) \cdot 64) \cdot \xi_1 \\ &\quad + ((4 \cdot 64 + 0) \cdot 64 + 3) \cdot 64 + 2, 23) \\ &= (((((-4 \cdot 64 + 1) \cdot 23 + 0)) \cdot 23 + (-7 \cdot 64 + 3) \cdot 64) \cdot 23 \\ &\quad + ((4 \cdot 64 + 0) \cdot 64 + 3) \cdot 64 + 2 \end{aligned}$$

First step: apply Horner's schema to coefficient list $d \in \text{DIO}$ und (trailing) Argument x_2 : indeterminate ξ_1 is coded by list nesting and is seen as a *constant*, as an element of intermediate ring $\mathbb{Z}[\xi_1]$:

$$\mathbb{Z}[\xi_1, \xi_2] \stackrel{\text{by def}}{=} \mathbb{Z}[\xi_1][\xi_2] \stackrel{\text{by def}}{=} (\mathbb{Z}[\xi_1])[\xi_2].$$

Last—here second—step: evaluation of $\mathbb{Z}[\xi_1]$ polynomial in remaining indeterminate ξ_1 on remaining argument x_1 , by a last application of Horner's schema.

3 Arithmetical frame theories

We consider here as frame theories—for our decision algorithm – **on one hand** classically quantified arithmetical theories $\mathbf{T} = \mathbf{Q} + \mathbf{AC}$ with (countable) axiom of choice, as in particular Zermelo-Fraenkel set theory $\mathbf{T} = \mathbf{ZFC} = \mathbf{ZF} + \mathbf{AC}$. Frame then is the strengthening

$$\mathbf{T}^+ = \mathbf{T} + \text{Con}_{\mathbf{T}} = \mathbf{ZFC} + \text{Con}_{\mathbf{ZFC}}$$

of \mathbf{T} by its own consistency-*formula*

$$\begin{aligned}\text{Con}_{\mathbf{T}} &= \neg(\exists k \in \mathbb{N}) \text{Prov}_{\mathbf{T}}(k, \ulcorner \text{false} \urcorner) \\ &= (\forall k) \neg \text{Prov}_{\mathbf{T}}(k, \ulcorner \text{false} \urcorner) \text{ (Gödel)},\end{aligned}$$

see SMORYNSKI 1977 and op. cit.

Strengthening by this consistency formula will provide for *correctness* of our *decision process* (Hilbert).

On the other hand we take as frame the Free-Variables (categorical) theory $\mathbf{T} = \mathbf{PR} = \mathbf{PRa}$ of *Primitive Recursion with predicate abstraction into subsets*

$$(\chi = \chi(a) : A \rightarrow 2) \mapsto \{A : \chi\} = \{a \in A : \chi(a)\}$$

out of op. cit., $\mathbf{T} = \mathbf{S}$ in Smorynski's notation, as well as *descent theory* $\pi\mathbf{R} = \pi\mathbf{R}^+ = \pi\mathbf{R} + \text{Con}_{\pi\mathbf{R}}$: that theory is self-consistent, $\pi\mathbf{R} \vdash \text{Con}_{\pi\mathbf{R}}$, main result of op. cit.

4 A μ -recursive race for decision

We **define** an enumerative *race*—for $d \in \text{DIO}$ thought *passive*, *fixed*, and $k \in \mathbb{N}$ *running*—for satisfaction of

$$\begin{aligned}\varphi_0(d, k) &= [\text{ev}(d, \text{ct}_* k) = 0] \text{ against} \\ \varphi_1(d, k) &= \text{Prov}_{\mathbf{T}}(k, \ulcorner (\vec{x})\text{ev}(d, \vec{x}) \neq 0 \urcorner) : \text{DIO} \times \mathbb{N} \rightarrow 2 = \{0, 1\}, \\ \text{ct}_* &= \text{ct}_* k : \mathbb{N} \xrightarrow{\cong} \mathbb{Z}^{(*)} \text{ Cantor-type count, } \vec{x} \in \mathbb{Z}^* \text{ free under code.}\end{aligned}$$

This race towards *termination* is defined as a—formally partial— μ -recursive mapping as follows within the theory $\hat{\mathbf{T}}$ of *partial PR maps*, i. e. of (partially defined) μ -recursive maps, cf. again op. cit.:

$$t = t(d) = \mu\{k \mid \varphi_0(d, k) \vee \varphi_1(d, k)\} : \text{DIO} \rightarrow \mathbb{N}. \quad (*)$$

Decision candidate then is

$$\begin{aligned} \nabla d &= \begin{cases} 0 & \text{if } \varphi_0(d, t(d)) \\ 1 & \text{if } \varphi_1(d, t(d)) \end{cases} \\ &= \begin{cases} 0 & \text{if } \text{ev}(d, \text{ct}_*(t(d))) = 0 \\ & \text{(zero found)} \\ 1 & \text{if } \text{Prov}_{\mathbf{T}}(t(d), \ulcorner \text{ev}(d, \vec{x}) \neq 0 \urcorner) \\ & \text{(internal proof found for global non nullity)} \end{cases} \\ &: \text{DIO} \xrightarrow{(\text{id}, t)} \text{DIO} \times \mathbb{N} \rightarrow \mathbb{2}. \end{aligned}$$

Question: Is ∇ *well-defined* as a partial map? In which frame?

Well-definedness of the decision within $\mathbf{T}^+ = \mathbf{ZFC}^+ = \mathbf{ZFC} + \text{Con}_{\mathbf{ZFC}} = \mathbf{T} + \text{Con}_{\mathbf{T}}$:

$$\begin{aligned} \mathbf{T}^+ &\vdash \varphi_0(d, k) \wedge \varphi_1(d, k') \\ &\quad \text{(cases-overlap Assumption)} \\ &\implies \text{ev}(d, \text{ct}_*k) = 0 \\ &\quad \wedge \text{Prov}_{\mathbf{T}}(k', \ulcorner (\vec{x}) \text{ev}(d, \vec{x}) \neq 0 \urcorner) \\ &\implies \text{Prov}_{\mathbf{T}}(j(k, k'), \ulcorner \text{false} \urcorner) \\ &\implies \neg \text{Con}_{\mathbf{T}} \implies \text{false}, \\ &j = j(k, k') : \mathbb{N}^2 \rightarrow \mathbb{N} \text{ suitable.} \end{aligned}$$

Consequence:

$$\mathbf{T}^+ \vdash \neg [\varphi_0(d, k) \wedge \varphi_1(d, k')] : \text{DIO} \times \mathbb{N}^2 \rightarrow \mathbb{2},$$

$\nabla = \nabla_{\mathbf{T}}(d) : \text{DIO} \rightarrow \mathbb{N}$ is *well-defined* as a (*formally partial*) μ -recursive map, within $\mathbf{T}^+ = \mathbf{T} + \text{Con}_{\mathbf{T}}$.

Well-definedness of decision within *descent* theory $\pi\mathbf{R}$:

We consider now *descent theory* $\pi\mathbf{R}$ out of op.cit. strengthening \mathbf{PR} by axiom (π) of *non-infinite endo driven descending complexity with complexity values in polynomial semiring* $\mathbb{N}[\omega]$, and its logical properties, in particular *soundness* giving $\pi\mathbf{R} \vdash \text{Con}_{\pi\mathbf{R}}$.

Decision $\nabla = \nabla_{\pi\mathbf{R}}(d) : \text{DIO} \rightarrow \mathbb{2}$ is in fact well-defined as a partial PR map, within theory $\pi\mathbf{R}$, since—in parallel to the above case $\mathbf{T} = \mathbf{ZFC}$:

$$\begin{aligned}
\pi\mathbf{R} &\vdash \varphi_0(d, k) \wedge \varphi_1(d, k') \\
&\quad (\text{cases-overlap Assumption}) \\
&\implies \text{ev}(d, \text{ct}_*k) = 0 \\
&\quad \wedge \text{Prov}_{\pi\mathbf{R}}(k', \ulcorner (\vec{x}) \text{ev}(d, \vec{x}) \neq 0 \urcorner) \\
&\implies \text{Prov}_{\pi\mathbf{R}}(j(k, k'), \ulcorner \text{false} \urcorner) \\
&\implies \text{“}\neg \text{Con}_{\pi\mathbf{R}}\text{”} \implies \text{false}, \\
&j = j(k, k') : \mathbb{N}^2 \rightarrow \mathbb{N} \text{ suitable.}
\end{aligned}$$

The latter since $\pi\mathbf{R} \vdash \text{Con}_{\pi\mathbf{R}}$.

Well-definedness of DIO-decision within PR itself

Decision $\nabla = \nabla_{\mathbf{PR}}(d) : \mathbf{DIO} \rightarrow \mathbb{2}$ is well-defined as a partial PR map, within theory $\widehat{\mathbf{PRa}}$ of partial PR maps since

$$\begin{aligned}
\widehat{\mathbf{PRa}} &\vdash \varphi_0(d, k) \wedge \varphi_1^{\mathbf{DIO}}(d, k') \\
&\quad (\text{cases-overlap Assumption}) \\
&\iff \text{ev}(d, \text{ct}_* k) = 0 \\
&\quad \wedge \text{Prov}_{\mathbf{DIO}}(k', \ulcorner (\vec{x}) \text{ev}(d, \vec{x}) \neq 0 \urcorner) \\
&\implies \text{Prov}_{\mathbf{DIO}}(j(k, k'), \ulcorner \text{false} \urcorner) \\
&\implies \text{false}, \\
&\quad j = j(k, k') : \mathbb{N}^2 \rightarrow \mathbb{N} \text{ suitable.}
\end{aligned}$$

The latter by *diophantine soundness* of $\mathbf{T} = \mathbf{PR}$, see SMORYNSKI 1977, THEOREM 4.1.4.

5 Decision Correctness

Decision Correctness, result-0-case:

$$\begin{aligned}
\mathbf{T} &\vdash [\varphi_0(d, t(d)) \implies \text{ev}(d, \text{ct}_* \circ t(d)) = 0] \\
&\subseteq \text{true}_{\mathbf{DIO}} : \mathbf{DIO} \xrightarrow{(\text{id}, t)} \mathbf{DIO} \times \mathbb{N} \rightarrow \mathbb{2} :
\end{aligned}$$

If race-for-decision ∇ *terminates* on DIO-code d , with **result** 0, **then** (evaluation of) d has (at least) one zero, namely

$$\text{ct}_* \circ t(d) \in \mathbb{N}.$$

Correctness, result-1-case:

$$\begin{aligned}
\mathbf{T} \vdash \varphi_1(d, k) &\implies \text{Prov}_{\mathbf{DIO}}(k, \ulcorner \text{ev}(d, \vec{x}) \neq 0 \urcorner) \\
&\implies \text{ev}(d, \vec{x}) \neq 0 : (\mathbf{DIO} \times \mathbb{N}) \times \mathbb{Z}^* \rightarrow \mathbb{2}, \\
&\quad (d \in \mathbf{DIO}, k \in \mathbb{N}, \vec{x} \in \mathbb{Z}^* \text{ all free}), \\
&\quad \text{or, with quantifier decoration:} \\
\mathbf{T} \vdash (\forall d \in \mathbf{DIO})(\forall k \in \mathbb{N})(\forall \vec{x} \in \mathbb{Z}^*) \\
&\quad [\varphi_1^{\mathbf{T}}(d, k) \implies \text{Prov}_{\mathbf{DIO}}(k, \ulcorner \text{ev}(d, \vec{x}) \neq 0 \urcorner) \\
&\quad \implies \text{ev}(d, \vec{x}) \neq 0].
\end{aligned}$$

If race-for-decision ∇ *terminates* on DIO-code d , with **result** 1, **then** (evaluation of) d has no zeroes.

This because of *Diophantine Soundness* of \mathbf{T} , see SMORYN-SKI 1977, THEOREM 4.1.4 again.

Correctness in result-1-case, under termination condition:

Substitution of $t(d)$ for k in the above gives

$$\begin{aligned}
\mathbf{T}^+, \pi \mathbf{R}, \mathbf{PR} \vdash [\varphi_1^{\mathbf{DIO}}(d, t) \implies \text{ev}(d, \vec{x}) \neq 0] &\subseteq \text{true}_{\mathbf{DIO} \times \mathbb{Z}^*}, \\
&\quad d \in \mathbf{DIO}, \vec{x} \in \mathbb{Z}^* \text{ both free :}
\end{aligned}$$

Correctness of $\nabla(d)$ where defined, in *both* defined cases: in case of reaching **result** 0, as well as in case of reaching **result** 1.

[For partial maps $f, g : A \multimap B$, $f \subseteq g$ designates *inclusion* of the *graphs* of f and g .]

6 Termination

We show first

Pointwise non-derivability of non-termination:

For no diophantine *point* $d_0 : \mathbb{1} \rightarrow \text{DIO}$ \mathbf{T} derives non-termination of t at d_0 .

Proof:

Assumption

$$\begin{array}{c} \mathbf{T} \vdash (\vec{x})\text{ev}(d_0, \vec{x}) \neq 0 \quad (\bullet) \\ \wedge (k) \neg \text{Prov}_{\mathbf{T}}(k, \ulcorner (\vec{x})\text{ev}(d_0, \vec{x}) \neq 0 \urcorner) \\ \hline \mathbf{T} \vdash \text{Prov}_{\mathbf{T}}(\text{num } \underline{j}, \ulcorner (\vec{x})\text{ev}(d_0, \vec{x}) \neq 0 \urcorner) \\ \wedge (k) \neg \text{Prov}_{\mathbf{T}}(k, \ulcorner (\vec{x}) D(\vec{x}) \neq_Z 0 \urcorner) \end{array}$$

a contradiction: appropriate \underline{j} is available from (\bullet) via derivation-to-Proof-internalisation (*gödelisation*).

[For the time being we consider \mathbf{T} as frame, not (yet) $\mathbf{T}^+ = \mathbf{T} + \text{Con}_{\mathbf{T}}$.]

For $\mathbf{T} = \mathbf{Q}$ quantified, with (countable) *axiom of choice* **ACC**, in particular $\mathbf{Q} = \mathbf{PA} + \mathbf{ACC}$ Peano Arithmetic with choice, we define the *undecided part* of DIO as

$$\begin{aligned} \Psi &= \Psi^{\mathbf{Q}} \\ &= \{d \in \text{DIO} : \forall k \text{ev}(d, \text{ct}_* k) \neq 0 \\ &\quad \wedge \forall k \neg \text{Prov}_{\mathbf{Q}}(k, \ulcorner (\vec{x})\text{ev}(d, \vec{x}) \neq 0 \urcorner)^\top\} \\ &\subset \text{DIO} = \mathbb{Z}^{(*)} \subset \mathbb{N}. \end{aligned}$$

With this definition we get

$$\begin{aligned} \mathbf{Q} \vdash \Psi \neq \emptyset &\implies \text{choice}_{\Psi} : \mathbb{1} \rightarrow \Psi \subset \mathbb{N} \text{ total} \\ &(\text{choice available by } \mathbf{ACC} : \text{non-empty sets have } \textit{defined points}) \\ &\implies \mu\{d : t(d) \text{ non-terminating}\} : \mathbb{1} \rightarrow \Psi \text{ total}. \end{aligned}$$

This means: the assumption of (formal) *existence* of a $d \in \text{DIO}$ for which decision race $t : \text{DIO} \rightarrow \mathbb{N}$ does *not* terminate, leads to a (*defined*) point

$$d_0 : \mathbb{1} \rightarrow \text{DIO}$$

for which t derivably does not terminate.

But this is **excluded** by pointwise non-derivability above of non-termination, within frame \mathbf{Q} assumed consistent.

So we have shown

$$\begin{aligned} \mathbf{Q}, \mathbf{PA} + \mathbf{ACC} &\vdash \Psi = \emptyset, \text{ i. e.} \\ \mathbf{Q} &\vdash (\forall d \in \mathbf{DIO}) [\exists k \text{ ev}(d, \text{ct}_*k) = 0 \\ &\quad \vee \exists k \text{ Prov}_{\mathbf{DIO}}(k, \ulcorner (\vec{x}) \text{ ev}(d, \vec{x}) \urcorner) \neq 0], \end{aligned}$$

whence

Termination Theorem: $\mathbf{Q}, \mathbf{ZFC}, \mathbf{PA} + \mathbf{ACC}$ derive race t to terminate on all diophantine codes d , on all $d \in \mathbf{DIO} = \mathbb{Z}^{(*)}$.

7 Correct termination of decision ∇

In particular $(\mathbf{Q}^+ = \mathbf{Q} + \mathbf{ACC}$ stronger than \mathbf{Q}):

\mathbf{Q}^+ derives

overall termination of μ -recursive

termination race $t = t^{\mathbf{Q}}(d) : \mathbf{DIO} \rightarrow \mathbb{N} :$

$$\mathbf{Q}^+ \vdash [(\forall d \in \mathbf{DIO}) t(d) \in \mathbb{N} \text{ defined}]$$

Hence, by Decision Correctness within $\mathbf{Q}^+ :$

\mathbf{Q}^+ derives

overall *correct* termination of μ -recursive *decision*

$\nabla : \mathbf{DIO} \rightarrow 2$, **main result** here:

$$\begin{aligned} &\nabla(d) \\ &= \begin{cases} 0 & \text{if } \text{ev}(d, t(d)) = 0 \\ & [\implies d \text{ has a zero } \vec{z} \in \mathbb{Z}^*] \\ 1 & \text{if } \text{Prov}_{\mathbf{DIO}}(t, \ulcorner (\forall \vec{x}) \text{ ev}(d, \vec{x}) \neq 0 \urcorner) \\ & [\implies d \text{ has no zero }] \end{cases} : \mathbf{DIO} \rightarrow 2. \end{aligned}$$

8 Comparison with Matiyasevich's negative result

Main result above says in terms of the theory **TM** of TURING machines, by the established part of CHURCH's thesis:

For concrete diophantine polynomials $D = D(\vec{x}) : \mathbb{Z}^m \rightarrow \mathbb{Z}$:

For quantified arithmetical choice theories **Q** + **ACC** like **ZFC** and already **PA** + **ACC**,

Q⁺ = **Q** + Con_{**Q**} **derives**:

TURING machine $\text{TM}_{\nabla_{\mathbf{Q}}}$ corresponding—CHURCH—to totally defined μ -recursive decision map

$$\nabla_{\mathbf{Q}} : \text{DIO} \rightarrow \{0, 1\},$$

when written coefficient list $\lfloor D \rfloor$ of a diophantine polynomial D on its (initial) TAPE, eventually **reaches** HALT state, leaves result 0 (as its final TAPE) **iff** D has a zero $\vec{z} : D(\vec{z}) = 0$, and **result** 1 **iff** D is overall non-null: $(\forall \vec{x} \in \mathbb{Z}^*) [D(\vec{x}) \neq 0]$.

This contradicts **Matiyasevich's THEOREM** *unsolving* Hilbert's 10th problem, within theory **Q**⁺ which strengthens his framework of Peano Arithmetic **PA** + **ACC** with countable axiom of choice. Whence

Conclusion:

- **ZFC**⁺ = **ZFC** + Con_{**ZFC**} is contradictory, so
- **ZFC** $\vdash \neg$ Con_{**ZFC**} : **ZFC** is internally inconsistent,
- same for theory **PA** + **ACC** :

Peano-Arithmetic with axiom of countable choice is internally inconsistent

- **Question:** is already Peano Arithmetic **PA** by itself internally inconsistent? It would be if axiom **ACC** of countable choice were derivable within **PA** or independent from **PA**, as is axiom of choice **AC** from **set** theory. This would mean that formal existential quantification is incompatible with free-variables Primitive Recursive Arithmetic **PR**.

Discussion

- After his talk at Humboldt University Berlin, I have mailed to Matiyasevich the question, if his *unsolving* of Hilbert's 10th problem is really constructive: it depends heavily on formal existential quantification. No reply: may be he considers this question when present paper will be brought to his attention.
- I have submitted the 200? version of present work, claiming self-inconsistency $\mathbf{PA} \vdash \neg \text{Con}_{\mathbf{PA}}$, to the *Journal of Symbolic Logic*. The (anonymous) referee:
... *this is certainly false*. ... Robert 'Rob' GOLDBLATT ed.: *under these circumstances etc.*

What is such editorial policy good for?

9 Hilbert 10 constructively

In this section we show that the *local* version $\nabla[D] : 1 \rightarrow 2$ of the μ -recursive *decision algorithm* $\nabla = \nabla_{\text{DIO}}(d) : \text{DIO} \rightarrow 2$ *irrefutably decides each (single) diophantine equation—correctly—* when placed in p. r. *non-infinite-descent theory* $\pi\mathbf{R} = \mathbf{PR} + (\pi)$ of op. cit. in the References.

This will give a positive solution to Hilbert's 10th problem in that constructive framework, at least when stated in its original form quoted in first section above.

Formally, this **problem** allows for solution by a separate decision algorithm (“process”) for each diophantine polynomial. By *localisation* at a given polynomial, we extract such a decision-*family* from the forgoing sections, and formalise it within $\pi\mathbf{R}$.

We index that family (externally) by the *diophantine constants* $\delta : \mathbb{1} \rightarrow \text{DIO} \subset \mathbb{N}$, among which the diophantine polynomials

$$D = D(\vec{x}) = D(x_1, \dots, x_m) : \mathbb{Z}^m \rightarrow \mathbb{Z}$$

are represented by their coefficient list codes $\lfloor D \rfloor : \mathbb{1} \rightarrow \text{DIO}$.

Definition: For PR predicates $\varphi_0, \varphi_1 : A \times \mathbb{N} \rightarrow \mathbb{2}$ we define the *race winner predicate*

$$\mu_{\vee}[\varphi_0, \varphi_1] : A \rightarrow \mathbb{2}$$

between φ_0 and φ_1 slightly asymmetrically by

$$\begin{aligned} \mu_{\vee}[\varphi_0, \varphi_1] &= \mu_{\vee}[\varphi_0, \varphi_1](a) \\ &=_{\text{def}} (dc \circ (\varphi_0, \varphi_1)) \hat{\circ} (A \times \mu[\varphi_0 \vee \varphi_1]) \hat{\circ} \Delta_A : \\ A &\rightarrow A \times A \rightarrow A \times \mathbb{N} \rightarrow \mathbb{2} \times \mathbb{2} \xrightarrow{dc} \mathbb{2}, \text{ with} \\ dc &= dc(u, v) : \mathbb{2} \times \mathbb{2} \rightarrow \mathbb{2} \text{ defined by} \\ dc(u, v) &=_{\text{def}} \begin{cases} 0 & \text{if } u = 1, \\ 1 & \text{if } u = 0 \wedge v = 1, \\ \text{definably undefined} & \text{if } u = v = 0. \end{cases} \end{aligned}$$

This (partial) race winner predicate $\mu_{\vee}[\varphi_0, \varphi_1](a) : A \rightarrow \mathbb{2}$ is characterised—within $\mathbf{S} = \mathbf{PR}$ as well as in $\mathbf{S} = \pi\mathbf{R}$ —by

$$\begin{aligned} \mathbf{S} \vdash [\varphi_0(a, n) \wedge \bigwedge_{i < n} \neg \varphi_1(a, n) \implies \mu_{\vee}[\varphi_0, \varphi_1](a) = 0] \\ \wedge [\varphi_1(a, n) \wedge \bigwedge_{i \leq n} \neg \varphi_0(a, n) \implies \mu_{\vee}[\varphi_0, \varphi_1](a) = 1]. \end{aligned}$$

We allow us to write for this intuitively—in classical terms of a (partial) case-distinction:

$$\mu_{\vee}[\varphi_0, \varphi_1](a) = \begin{cases} 0 & \text{if } \mu\varphi_0(a) < \infty \wedge \mu\varphi_0(a) \leq \mu\varphi_1(a), \\ 1 & \text{if } \mu\varphi_1(a) < \infty \wedge \mu\varphi_1(a) < \mu\varphi_0(a). \end{cases}$$

Our decision family

$$\nabla[\delta] : 1 \rightarrow 2, \quad \delta : 1 \rightarrow \text{DIO} \subset \mathbb{N}$$

now is defined in the present μ -recursive frame as this type of race winning, of PR search for a zero (in the evaluation) of δ against PR search for a (first) internal non-nullity *proof* for (the evaluation) of δ , namely by

$$\begin{aligned} \nabla[\delta] &=_{\text{def}} \mu_{\vee}[\varphi_0[\delta], \varphi_1[\delta]] : 1 \rightarrow 2, \text{ with} \\ \varphi_0[\delta](k) &=_{\text{def}} [\text{ev}(\delta, \text{ct}_*(k)) = 0] : \mathbb{N} \rightarrow 2, \\ \varphi_1[\delta](k) &=_{\text{def}} \text{Prov}_{\mathbf{S}}(k, \ulcorner (\vec{x})\text{ev}(\delta, \vec{x}) \neq 0 \urcorner). \end{aligned}$$

Here

$$\text{ev} = \text{ev}(d, x) : \mathbb{N} \times \mathbb{N} \supset \text{DIO} \times \mathbb{Z}^* \rightarrow \mathbb{Z}$$

is evaluation with the characteristic **evaluation property**

$$\text{ev}(\ulcorner D \urcorner, (x_1, \dots, x_m)) = D(x_1, \dots, x_m) : Z^m \rightarrow \mathbb{Z},$$

realised by (iterated) HORNER’s schema (each application reduces the number of remaining variables by 1), or by “brute force” evaluation of monomials.

9.1 Decision Correctness

Soundness Recall: Main result of op.cit. in the References is (logical) *soundness* of theory $\pi\mathbf{R}$:

- For a (p. r.) predicate $\chi = \chi(a) : A \rightarrow \mathbb{2}$ we have

$$\pi\mathbf{R} \vdash \text{Prov}_{\pi\mathbf{R}}(k, \ulcorner \chi \urcorner) \implies \chi(a) : \mathbb{N} \times A \rightarrow \mathbb{2},$$

$a \in A$ free, meaning here *for all* $a \in A$, and $k \in \mathbb{N}$ free, meaning here *exists* $k \in \mathbb{N}$. This entails

- **PR soundness** of $\pi\mathbf{R}$: For a p. r. predicate $\chi = \chi(a) : A \rightarrow \mathbb{2}$,

$$\pi\mathbf{R} \vdash \text{Prov}_{\mathbf{PR}}(k, \ulcorner \chi \urcorner) \implies \chi(a) : \mathbb{N} \times A \rightarrow \mathbb{2},$$

as well as in particular

- *Diophantine soundness* of $\pi\mathbf{R}$: for a diophantine polynomial $D = D(\vec{x}) : \mathbb{Z}^* \rightarrow \mathbb{2}$

$$\pi\mathbf{R} \vdash \text{Prov}_{\pi\mathbf{R}}(k, \ulcorner (\vec{x})D(\vec{x}) \neq 0 \urcorner) \implies D(\vec{x}) \neq 0,$$

$k \in \mathbb{N}$, $\vec{x} \in \mathbb{Z}^*$ free.

- Already $\mathbf{PR}^+ = \mathbf{PR} + \text{Con}_{\mathbf{PR}}$ is diophantine sound. This needs an extra Proof.

We consider here frame $\mathbf{S} = \pi\mathbf{R}$,

$$\pi\mathbf{R}^+ = \pi\mathbf{R} + \text{Con}_{\pi\mathbf{R}} = \pi\mathbf{R},$$

the latter by op.cit. equivalent to soundness of theory $\pi\mathbf{R}$.

Namely from PR Soundness we get the

Local Correctness-Lemma for $\nabla[\delta]$ in $\pi\mathbf{R}$: The partial \mathbf{PR} -map $\nabla[\delta] : \mathbb{1} \rightarrow \mathbb{2}$ has the following correctness properties:

$\pi\mathbf{R} \vdash :$

- δ does not fall in *both* of the two defined-cases stated for $\nabla[\delta]$,

- $\nabla[\delta] = 0 \implies \text{ev}(\delta, \text{ct}_* \circ \mu\varphi_0[\delta]) = 0$: δ is implied to have available a zero in its *evaluation*,
- $\nabla[\delta] = 1 \implies \text{ev}(\delta, \vec{x}) \neq_Z 0$, \vec{x} free in \mathbb{Z}^* : δ is implied to be evaluated globally non-null, in particular:
- By diophantine evaluation for $D = D(x_1, \dots, x_{\mathbf{m}}) : \mathbb{Z}^* \rightarrow \mathbb{Z}$ diophantine:
 - $\nabla[D] := \nabla[\ulcorner D \urcorner] = 0 \implies D(\text{ct}_*(\mu\varphi_0[\ulcorner D \urcorner])) = 0$:
 D is implied to have a zero, as well as
 - $\nabla[D] = 1 \implies [D(\vec{x}) \neq 0]$, here again \vec{x} free over \mathbb{Z}^* :
 D is implied to be globally non-null **q.e.d.**

9.2 Decision Termination

The final question to treat for this—canonical—family

$$\nabla = \nabla_{\mathbf{DIO}}[\delta] : \mathbb{1} \rightarrow \mathbb{2}, \delta : \mathbb{1} \rightarrow \mathbf{DIO} \subset \mathbb{N}$$

of *local*— μ -recursive—decision algorithms, is *termination*, for each δ , in particular for $\delta = \ulcorner D \urcorner$, $D = D(\vec{x})$ diophantine.

Assume $\nabla[d_0]$ *not* to terminate for a particular *constant* $d_0 : \mathbb{1} \rightarrow \mathbf{DIO}$, in particular d_0 of form $D_0 = D_0(\vec{x})$.

Since we argue here purely *syntactically*—within the *theory* $\widehat{\mathbf{S}} \supset \mathbf{S} = \mathbf{PR} + (\text{abstr})$ of *partial* p.r. maps—no modelling in mind except some primitive recursive *Metamathematics* (these in turn gödelised within \mathbf{S})—we discuss the stronger assumption

$\nabla[d_0]$ **T-derivably** does *not* terminate for a given diophantine constant $d_0 : \mathbb{1} \rightarrow \mathbf{DIO}$, **T** an extension of \mathbf{S} .

This **assumption** reads:

$$\mathbf{T} \vdash (k)\psi[d_0](k) :$$

here k is free over \mathbb{N} , and the PR predicate $\psi[d_0](k) : \mathbb{N} \rightarrow \mathbb{2}$ is defined by

$$\begin{aligned}\psi[d_0](k) &= \psi_0[d_0](k) \wedge \psi_1[d_0](k) \text{ with} \\ \psi_0[d_0](k) &= [\text{ev}(d_0, \text{ct}_*(k)) \neq 0], \text{ and} \\ \psi_1[d_0](k) &= \neg \text{Prov}_{\mathbf{T}}(k, \ulcorner \text{ev}(d_0, \vec{x}) \neq 0 \urcorner).\end{aligned}$$

So the assumption (“of the contrary”) reads:

$$\begin{aligned}\mathbf{T} \vdash & [\text{ev}(d_0, \text{ct}_*(k)) \neq 0] \\ & \wedge \neg \text{Prov}_{\mathbf{T}}(k, \ulcorner (\vec{x})\text{ev}(d_0, \vec{x}) \neq 0 \urcorner).\end{aligned}$$

Here $k \in \mathbb{N}$ is the only free variable in the *accessible* level, \vec{x} is free over \mathbb{Z}^* , but *encapsulated* within gödelisation, *not visible* on the object language level.

The derivably-non-termination assumption

$$\mathbf{T} \vdash \psi[d_0](k), \text{ } k \text{ free,}$$

would entail in particular (first conjunct $\psi_0[d_0]$):

$$\mathbf{T} \vdash \text{ev}(d_0, \text{ct}_*(k)) \neq 0 : \mathbb{N} \rightarrow \mathbb{2}.$$

Internalising (formalising) this metamathematical statement, we (would) get by Proof-Internalisation—cf. SMORYNSKI 1977—a *constant* $p_0 : \mathbb{1} \rightarrow \text{Proof}_{\mathbf{T}} \subset \mathbb{N}$ *guilty* for this last statement:

$$\mathbf{T} \vdash \text{Prov}_{\mathbf{T}}(p_0, \ulcorner \text{ev}(d_0, \vec{x}) \neq 0 \urcorner);$$

this would give, by definition of $\nabla[d_0]$:

$$\mathbf{T} \vdash \nabla[d_0] = 1,$$

a contradiction to our assumption that d_0 be derivably *not decided* by $\nabla_{\mathbf{DIO}}$, i. e. to $\mathbf{T} \vdash \psi[d_0]$.

Conclusion:

- $\pi\mathbf{R} = \pi\mathbf{R} + \text{Con}_{\pi\mathbf{R}}$ derives the alleged decision algorithm (family) $\nabla = \nabla_{\mathbf{DIO}}[D] : \mathbb{1} \rightarrow \mathbb{2}$ to be *correct* for each diophantine polynomial (if defined).
- no diophantine polynomial $D = D(\vec{x})$ can come with a \mathbf{T} -proof (i. p. a $\pi\mathbf{R}$ -proof) showing $\nabla[D]$ to be *undefined*, *not* to terminate, in other words:
- *correct termination* of the μ -recursive *decision family* $\nabla = \nabla_{\mathbf{DIO}}[D]$ at each diophantine polynomial is $\pi\mathbf{R}$ -*irrefutable*, in the sense that **otherwise**—refutation—

$\pi\mathbf{R} \vdash \text{Prov}_{\pi\mathbf{R}}(q, \ulcorner \text{false} \urcorner)$, $q : \mathbb{1} \rightarrow \mathbb{N}$ a suitable PR point,

inconsistency of (self-consistent) theory $\pi\mathbf{R}$ would be the consequence.

Outlook

Irrefutable correct termination of *uniform* decision algorithm

$$\nabla_{\mathbf{DIO}} = \nabla_{\mathbf{DIO}}(d) : \mathbf{DIO} \rightarrow \mathbb{2}, \quad d \in \mathbf{DIO} \text{ free}$$

is treated within the general framework of

Arithmetical Decision to come.

References

- [1] J. BARWISE ed. 1977: *Handbook of Mathematical Logic*. North Holland.
- [2] K. GÖDEL 1931: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. der Mathematik und Physik* **38**, 173-198.
- [3] D. HILBERT 1970: Mathematische Probleme. Vortrag Paris 1900. *Gesammelte Abhandlungen*. Springer.

- [4] Y. V. MATIYASEVICH 1993: *Hilbert's Tenth Problem*. The MIT Press.
- [5] M. PFENDER 2014a: *Consistency Decision*, arXiv 2014.
- [6] M. PFENDER 2014b: *Arithmetical Foundations*, γ version, www3.tu-berlin.de/preprint/mathematik/Preprint-8-2014
- [7] C. SMORYNSKI 1977: The Incompleteness Theorems. Part D.1 in BARWISE ed. 1977.